Serval Rhizome Store-and-Forward
&
Serval Mesh Datagram Protocols

Dr. Paul Gardner-Stephen,
Flinders University.

Serval Project: quick intro

- Infrastructure independent mobile communications.
- Target: disaster response & community resilience.
- Security is a high priority.
  - Privacy laws, personal security always apply.
- Aspires to function in a global-scale network.
- Functioning prototype software including many of the features described in following slides. Try it out at:
  - Search for Serval Mesh on Google Play

IP unsuited to MANETs

- Internet topologies are comparatively stable, and lend themselves to route summarisation
- Network addresses are sedentary with regards to position in network topology.
- Internet per-hop packet loss probability is very low.
- Internet links are rarely broadcast radio.
- These assumptions do not hold for MANETs.

MANET challenges

- Highly dynamic network topology and associated network address migration: route summarising less useful.
- Position in network topology no longer indicates identity, affiliation or authorisation.
- Global routing information too large to synchronise.

An observation

- End-to-end routing sacrifices bandwidth to reduce latency.
- The overhead of synchronising routing grows super-linearly with network size.
- So why not just synchronise the data instead?
- Scale limit shifts from # of nodes to amount of data
- Especially effective when there are multiple consumers of the same data, e.g., maps and other information.
- Effectively provides infinite retry.

Another observation

- IP+IPsec is complex, and ultimately the binding between IP address and identity is imperfect.
- So why not just use public keys as network addresses?
  - Random addresses prevent route summarisation
  - Long keys/addresses add overhead, but address abbreviation is a possible solution.

Reinterpreting challenges as opportunities

- No need to allocate addresses based on network location.
  - Allows random address allocation (simplified deployment) ...
  - … which in turn allows use of public keys as network addresses (simplifies many things)
- Explore route-independent communications systems
  - Synchronise data instead of routes

Mesh Datagram Protocol (MDP)

- Connectionless protocol analogous to UDP.
- Public keys are used as network addresses “SIDs” (Serval IDs): no key exchange required.
- Addresses cannot be spoofed because packets are authenticated: no separate authentication required.
- Allows random self-allocation of addresses without fear of collision.
- Address abbreviation is used to reduce address overheads to less than that of IPv6 or even IPv4.

Serval Rhizome store-and-forward

- Dual-purpose file distribution protocol and simplex stream protocol.
- “bundles” instead of packets.
  - Bundle = meta-data + (possibly empty) file
- Leverages MDP to include strong authentication and encryption of payload.
- Delay tolerant through store-and-forward mechanism: flooded not routed.

Rhizome: File Distribution

- Files identified by cryptographic hash.
- File, recipient &/or sender can all be encrypted.
- Bundles are versioned: receiving a new version of a bundle will replace an older one.
- End-to-end SID-based encryption.
- Deletion of files by publishing new manifest with empty file.
- Auto-delete time can be set on bundles.
- Prioritising small bundles over big ones is an effective heuristic.

Rhizome: Streaming

- Simplex streams implemented through progressively growing bundles.
- Journal mode semantics allow for transfer only of new part of bundle file.
- Journal mode semantics allow for pruning of old part of bundle file once acknowledged.
- Strong eventual-delivery behaviour in return for relaxed latency (<1sec per hop for small journals).
- Used in Serval for SMS-like text messaging service.

Rhizome: Asymmetric & unconventional links

- As a bundle-based protocol Rhizome can use non-conventional links.
- Satellite downlink can be used to broadcast bundles to whole of theatre, with Rhizome replicating to those who missed the transmission.
- Physical transport of a device transports transmissions with it for replication to devices at the destination.
- Replication occurs automatically.

Strengths & Weaknesses

- We see strengths as including:
  - Resilient data delivery and distribution regardless of network topology, including when faced with partitioning. An implementation exists.
  - Excellent for distributing information *into* the network, and good for collecting information *out of* the network, e.g., command & control.
  - Excellent for sharing information *throughout* a mesh, e.g., situational awareness.

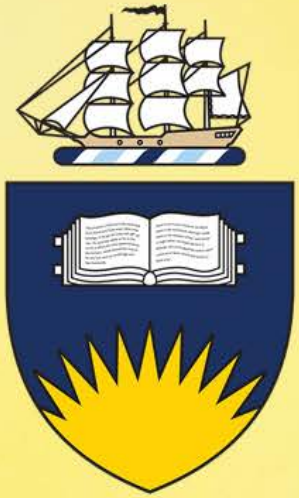
Strengths & Weaknesses

- We see challenges as including:
  - Traditional real-time point-to-point links hard in a large mesh
  - Large bundles (eg video) for a single recipient is grossly inefficient.
  - Extensive point-to-point communications *within* a large mesh may exceed network transmission and storage capacity: $O(n^2)$ conversations.

Suggested improvements

- Directed flooding / hybrid bundle + routing approaches, e.g., to funnel data out of the mesh, or to a single recipient without clogging all devices.
- Low TTL, geo-fencing, group labelling etc for localized point-to-point communications within a mesh without consuming resources elsewhere on the mesh.

Questions?



Flinders
UNIVERSITY

inspiring achievement